



全国计算机技术与软件专业技术资格（水平）考试指定用书

全国计算机技术与软件专业技术资格（水平）考试

信息安全工程师考试大纲

全国计算机专业技术资格考试办公室 编

清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试指定用书

**全国计算机技术与软件专业技术
资格（水平）考试**

信息安全工程师考试大纲

全国计算机专业技术资格考试办公室 编

清华大学出版社
北 京

内 容 简 介

本书是全国计算机专业技术资格考试办公室编写的信息安全工程师考试大纲。
本书还包括了人力资源和社会保障部、工业和信息化部的有关文件以及考试简介。

信息安全工程师考试大纲是针对本考试的中级资格制定的。
通过本考试的考生，可被用人单位择优聘任为工程师。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

图书在版编目(CIP)数据

信息安全工程师考试大纲/全国计算机专业技术资格考试办公室编. —北京：清华大学出版社，2016
全国计算机技术与软件专业技术资格（水平）考试指定用书
ISBN 978-7-302-43981-3

I. ①信… II. ①全… III. ①信息系统-安全技术-资格考试-考试大纲 IV. ①TP309-41

中国版本图书馆 CIP 数据核字（2016）第 120549 号

责任编辑：杨如林
封面设计：
责任校对：胡伟民
责任印制：

出版发行：清华大学出版社
网 址：http://www.tup.com.cn, http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 邮 编：100084
社 总 机：010-62770175 邮 购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者：
装 订 者：
经 销：全国新华书店
开 本：130mm×185mm 印 张：1.375 字 数：35 千字
版 次：2016 年 7 月第 1 版 印 次：2016 年 7 月第 1 次印刷
印 数：1~8000
定 价：15.00 元

产品编号：070140-01

前 言

全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）是由人力资源和社会保障部、工业和信息化部领导下的专业技术资格考试，属于国家职业资格考试。人事部、信息产业部联合颁发的国人部发[2003]39号文件规定了这种考试的政策。计算机软件考试包括了计算机软件、计算机网络、计算机应用、信息系统、信息服务等领域初级资格（技术员/助理工程师）、中级资格（工程师）、高级资格（高级工程师）的 27 种职业岗位。根据信息技术人才年轻化的特点和要求，报考这种资格考试不限学历与资历条件，以不拘一格选拔人才。现在，软件设计师、程序员、网络工程师、数据库系统工程师、系统分析师考试标准已经实现了中国与日本国互认，程序员和软件设计师考试标准已经实现了中国和韩国互认。

各种资格的考试大纲（考试标准）体现了相应职业岗位对知识与能力的要求。这些要求是由全国计算机专业技术资格考试办公室组织了全国相关企业、研究所、高校等许多专家，调研了很多相关企业的相应职业岗位，参考了先进国家的有关考试标准，逐步提炼，反复讨论形成的。一般的做法是先确定相应职业岗位的工作流程，对每个工作阶段又划分多个关键性活动，对每项活动再列出所需的知识以及所需的能力要求，最后，汇总这些知识要求与能力要求，形成考试大纲。初级与中级资格考试一般包括基础知识与应用技术两大科目；高级资格考试一般包括综合知识、案例分析与论文

三大科目。

正由于考试大纲来源于职业岗位的要求，是考试命题的依据，因此，这种考试已成为衡量考生是否具有职业岗位要求的一个检验标准，受到社会上各用人单位的广泛欢迎。20多年的考试历史也证明，这种考试已经成为我国著名的 IT 考试品牌，大批合格人员得到了升职聘用，对国家信息化发挥了重要的作用。这就是广大在职人员以及希望从事相关专业工作的学生积极报考的原因。

计算机软件考试的其他有关信息见网站 www.ruankao.org.cn 中的资格考试栏目。

编 者

2016 年 3 月

人 事 部 文 件 信 息 产 业 部

国人部发〔2003〕39号

关于印发《计算机技术与软件专业技术资格（水平）考试暂行规定》和《计算机技术与软件专业技术资格（水平）考试实施办法》的通知

各省、自治区、直辖市人事厅（局）、信息产业厅（局），国务院各部委、各直属机构人事部门，中央管理的企业：

为适应国家信息化建设的需要，规范计算机技术与软件专业人才评价工作，促进计算机技术与软件专业人才培养建设，人事部、信息产业部在总结计算机软件专业资格和水平考试实施情况的基础上，重新修订了计算机软件专业资格和水平考试有关规定。现将《计算机技术与软件专业技术资格（水平）考试暂行规定》和《计算机技术与软件专业技术资格（水平）考试实施办法》

印发给你们，请遵照执行。

自 2004 年 1 月 1 日起，人事部、原国务院电子信息系统推广应用办公室发布的《关于印发〈中国计算机软件专业技术资格和水平考试暂行规定〉的通知》（人职发〔1991〕6 号）和人事部《关于非在职人员计算机专业技术资格证书发放问题的通知》（人职发〔1994〕9 号）即行废止。

中华人民共和国
人 事 部

中华人民共和国
信 息 产 业 部

二〇〇三年十月十八日

计算机技术与软件专业技术资格（水平）考试暂行规定

第一条 为适应国家信息化建设的需要，加强计算机技术与软件专业人才培养，促进我国计算机应用技术和软件产业的发展，根据国务院《振兴软件产业行动纲要》以及国家职业资格证书制度的有关规定，制定本规定。

第二条 本规定适用于社会各界从事计算机应用技术、软件、网络、信息系统和信息服务等专业技术工作的人员。

第三条 计算机技术与软件专业技术资格（水平）考试（以下简称计算机专业技术资格（水平）考试），纳入全国专业技术人员职业资格证书制度统一规划。

第四条 计算机专业技术资格（水平）考试工作由人事部、信息产业部共同负责，实行全国统一大纲、统一试题、统一标准、统一证书的考试办法。

第五条 人事部、信息产业部根据国家信息化建设和信息产业市场需求，设置并确定计算机专业技术资格（水平）考试专业类别和资格名称。

计算机专业技术资格（水平）考试级别设置：初级资格、中级资格和高级资格 3 个层次。

第六条 信息产业部负责组织专家拟订考试科目、考试大纲和命题，研究建立考试试题库，组织实施考试工作和统筹规划培训等有关工作。

第七条 人事部负责组织专家审定考试科目、考试大纲和试题，会同信息产业部对考试进行指导、监督、检查，确定合格标准。

第八条 凡遵守中华人民共和国宪法和各项法律，恪守职业道德，具有一定计算机技术应用能力的人员，均可根据本人情况，报名参加相应专业类别、级别的考试。

第九条 计算机专业技术资格（水平）考试合格者，由各省、自治区、直辖市人事部门颁发人事部统一印制，人事部、信息产业部共同用印的《中华人民共和国计算机专业技术资格（水平）证书》。该证书在全国范围有效。

第十条 通过考试并获得相应级别计算机专业技术资格（水平）证书的人员，表明其已具备从事相应专业岗位工作的水平和能力，用人单位可根据《工程技术人員职务试行条例》有关规定和工作需要，从获得计算机专业技术资格（水平）证书的人员中择优聘任相应专业技术职务。

取得初级资格可聘任技术员或助理工程师职务；取

得中级资格可聘任工程师职务；取得高级资格，可聘任高级工程师职务。

第十一条 计算机专业技术资格（水平）实施全国统一考试后，不再进行计算机技术与软件相应专业和级别的专业技术职务任职资格评审工作。

第十二条 计算机专业技术资格（水平）证书实行定期登记制度，每3年登记一次。有效期满前，持证者应按有关规定到信息产业部指定的机构办理登记手续。

第十三条 申请登记的人员应具备下列条件：

- （一）取得计算机专业技术资格（水平）证书；
- （二）职业行为良好，无犯罪记录；
- （三）身体健康，能坚持本专业岗位工作；
- （四）所在单位考核合格。

再次登记的人员，还应提供接受继续教育或参加业务技术培训的证明。

第十四条 对考试作弊或利用其他手段骗取《中华人民共和国计算机专业技术资格（水平）证书》的人员，一经发现，即行取消其资格，并由发证机关收回证书。

第十五条 获准在中华人民共和国境内就业的外籍人员及港、澳、台地区的专业技术人员，可按照国家有关政策规定和程序，申请参加考试和办理登记。

第十六条 在本规定施行日前，按照《中国计算机软件专业技术资格和水平考试暂行规定》（人职发〔1991〕6号）参加考试并获得人事部印制、人事部和

信息产业部共同用印的《中华人民共和国专业技术资格证书》（计算机软件初级程序员、程序员、高级程序员资格）和原中国计算机软件专业技术资格（水平）考试委员会统一印制的《计算机软件专业水平证书》的人员，其资格证书和水平证书继续有效。

第十七条 本规定自 2004 年 1 月 1 日起施行。

计算机技术与软件专业技术资格（水平）考试实施办法

第一条 计算机技术与软件专业技术资格（水平）考试（以下简称计算机专业技术资格（水平）考试）在人事部、信息产业部的领导下进行，两部门共同成立计算机专业技术资格（水平）考试办公室（设在信息产业部），负责计算机专业技术资格（水平）考试实施和日常管理工作。

第二条 信息产业部组织成立计算机专业技术资格（水平）考试专家委员会，负责考试大纲的编写、命题、建立考试试题库。

具体考务工作由信息产业部电子教育中心（原中国计算机软件考试中心）负责。各地考试工作由当地人事行政部门和信息产业行政部门共同组织实施，具体职责分工由各地协商确定。

第三条 计算机专业技术资格（水平）考试原则上每年组织两次，在每年第二季度和第四季度举行。

第四条 根据《计算机技术与软件专业技术资格（水平）考试暂行规定》（以下简称《暂行规定》）第五

条规定，计算机专业技术资格（水平）考试划分为计算机软件、计算机网络、计算机应用技术、信息系统和信息服务 5 个专业类别，并在各专业类别中分设了高、中、初级专业资格考试，详见《计算机技术与软件专业技术资格（水平）考试专业类别、资格名称和级别层次对应表》（附后）。人事部、信息产业部将根据发展需要适时调整专业类别和资格名称。

考生可根据本人情况选择相应专业类别、级别的专业资格（水平）参加考试。

第五条 高级资格设：综合知识、案例分析和论文 3 个科目；中级、初级资格均设：基础知识和应用技术 2 个科目。

第六条 各级别考试均分 2 个半天进行。

高级资格综合知识科目考试时间为 2.5 小时，案例分析科目考试时间为 1.5 小时、论文科目考试时间为 2 小时。

初级和中级资格各科目考试时间均为 2.5 小时。

第七条 计算机专业技术资格（水平）考试根据各等级、各专业特点，采取纸笔、上机或网络等方式进行。

第八条 符合《暂行规定》第八条规定的人员，由本人提出申请，按规定携带身份证明到当地考试管理机构报名，领取准考证。凭准考证、身份证明在指定的时间、地点参加考试。

第九条 考点原则上设在地市级以上城市的大、中

专院校或高考定点学校。

中央和国务院各部门所属单位的人员参加考试，实行属地化管理原则。

第十条 坚持考试与培训分开的原则，凡参与考试工作的人员，不得参加考试及与考试有关的培训。

应考人员参加培训坚持自愿的原则。

第十一条 计算机专业技术资格（水平）考试大纲由信息产业部编写和发行。任何单位和个人不得盗用信息产业部名义编写、出版各种考试用书和复习资料。

第十二条 为保证培训工作健康有序进行，由信息产业部统筹规划培训工作。承担计算机专业技术资格（水平）考试培训的机构，应具备师资、场地、设备等条件。

第十三条 计算机专业技术资格（水平）考试、登记、培训及有关项目的收费标准，须经当地价格行政部门核准，并向社会公布，接受群众监督。

第十四条 考务管理工作要严格执行考务工作的有关规章和制度，切实做好试卷的命制、印刷、发送和保管过程中的保密工作，遵守保密制度，严防泄密。

第十五条 加强对考试工作的组织管理，认真执行考试回避制度，严肃考试工作纪律和考场纪律。对弄虚作假等违反考试有关规定者，要依法处理，并追究当事人和有关领导的责任。

附表（已按国人厅发[2007]139号文件更新）

计算机技术与软件专业技术 资格（水平）考试

专业类别、资格名称和级别对应表

资格 名称 级别 层次	专业 类别	计算机软件	计算机网络	计算机 应用技术	信息系统	信息服务
高级资格		信息系统项目管理师 系统分析师 系统架构设计师 网络规划设计师 系统规划与管理师				
中级资格		软件评测师 软件设计师 软件过程 能力评估师	网络工程师	多媒体应用 设计师 嵌入式系统 设计师 计算机辅助 设计师 电子商务设 计师	系统集成项 目管理工程 师 信息系统监 理师 信息安全工 程师 数据库系统 工程师 信息系统管 理工程师	计算机硬件 工程师 信息技术支 持工程师
初级资格		程序员	网络管理员	多媒体应用 制作技术员 电子商务技 术员	信息系统运 行管理员	网页制作员 信息处理技 术员

主题词：专业技术人员 考试 规定 办法 通知

抄送：党中央各部门、全国人大常委会办公厅、全国政协办公厅、国务院办公厅、高法院、高检院、解放军各总部。

人事部办公厅

2003 年 10 月 27 日印发

全国计算机软件考试办公室文件

软考办〔2005〕1号

关于中日信息技术考试标准 互认有关事宜的通知

各地计算机软件考试实施管理机构：

为进一步加强我国信息技术人才培养和选拔的标准化，促进国际间信息技术人才的流动，推动中日两国信息技术的交流与合作，信息产业部电子教育中心与日本信息处理技术人员考试中心，分别受信息产业部、人事部和日本经济产业省委托，就中国计算机技术与软件专业技术资格（水平）考试与日本信息处理技术人员考试（以下简称中日信息技术考试）的考试标准，于2005年3月3日再次签署了《关于中日信息技术考试标准互认的协议》，在2002年签署的互认协议的基础上增加了网络工程师和数据库系统工程师的互认。现就中日信息技术考试标准互认中的有关事宜内容通知如下：

一、中日信息技术考试标准互认的级别如下：

中国的考试级别 (考试大纲)	日本的考试级别 (技能标准)
系统分析师	系统分析师 项目经理 应用系统开发师
软件设计师	软件开发师
网络工程师	网络系统工程师
数据库系统工程师	数据库系统工程师
程序员	基本信息技术师

二、采取灵活多样的方式，加强对中日信息技术考试标准互认的宣传，不断扩大考试规模，培养和选拔更多的信息技术人才，以适应日益增长的社会需求。

三、根据国内外信息技术的迅速发展，继续加强考试标准的研究与更新，提高考试质量，进一步树立考试的品牌。

四、鼓励相关企业以及研究、教育机构，充分利用中日信息技术考试标准互认的新形势，拓宽信息技术领域国际交流合作的渠道，开展多种形式的国际交流与合作活动，发展对日软件出口。

五、以中日互认的考试标准为参考，引导信息技术领域的职业教育、继续教育改革，使其适应新形势下的职业岗位实际工作要求。

二〇〇五年三月八日

全国计算机软件考试办公室文件

软考办〔2006〕2号

关于中韩信息技术考试标准互认 有关事宜的通知

各地计算机软件考试实施管理机构：

为加强我国信息技术人才培养和选拔的标准化，促进国际间信息技术人才的流动，推动中韩两国间信息技术的交流与合作，信息产业部电子教育中心与韩国人力资源开发服务中心，分别受信息产业部和韩国信息通信部的委托，对中国计算机技术与软件专业技术资格（水平）考试与韩国信息处理技术人员考试（以下简称中韩信息技术考试）的考试标准进行了全面、认真、科学的分析比较，于2006年1月19日签署了《关于中韩信息技术考试标准互认的协议》，实现了程序员、软件设计师考试标准的互认，现将中韩信息技术考试标准互认的有关事宜通知如下：

一、中韩信息技术考试标准互认的级别如下：

中国的考试级别 (考试大纲)	韩国的考试级别 (技能标准)
软件设计师	信息处理工程师
程序员	信息处理产业工程师

二、各地应以中韩互认的考试标准为参考，积极引导信息技术领域的职业教育发展，使其适应新形势下的职业岗位的要求。

三、鼓励相关企业以及研究、教育机构，充分利用中韩信息技术考试标准互认的新形势，拓宽信息技术领域国际交流合作的渠道，开展多种形式的国际交流与合作活动，发展对韩软件出口。

四、根据国内外信息技术的迅速发展，加强考试标准的研究与更新，提高考试质量，进一步树立考试的品牌。

五、各地应采取灵活多样的方式，加强对中韩信息技术考试标准互认的宣传，不断扩大考试规模，培养和选拔更多的信息技术人才，以适应日益增长的社会需求。

二〇〇六年二月五日

全国计算机技术与软件专业技术 资格（水平）考试简介

全国计算机技术与软件专业技术资格（水平）考试（简称计算机软件考试）是在人力资源和社会保障部、工业和信息化部领导下的国家考试，其目的是，科学、公正地对全国计算机技术与软件专业技术人员进行职业资格、专业技术资格认定和专业技术水平测试。

计算机软件考试在全国范围内已经实施了二十多年，年考试规模已超过三十万人。该考试由于其权威性和严肃性，得到了社会及用人单位的广泛认同，并为推动我国信息产业特别是软件产业的发展和提高各类 IT 人才的素质做出了积极的贡献。

根据人事部、信息产业部文件（国人部发[2003]39号），计算机软件考试纳入全国专业技术人员职业资格证书制度的统一规划。通过考试获得证书的人员，表明其已具备从事相应专业岗位工作的水平和能力，用人单位可根据工作需要从获得证书的人员中择优聘任相应专业技术职务（技术员、助理工程师、工程师、高级工程师）。计算机技术与软件专业实施全国统一考试后，不再进行相应专业技术职务任职资格的评审工作。因

此，这种考试既是职业资格考试，又是专业技术资格考试。报考任何级别不需要学历、资历条件，考生可根据自己熟悉的专业情况和水平选择适当的级别报考。程序员、软件设计师、系统分析师、网络工程师、数据库系统工程师的考试标准已与日本相应级别实现互认，程序员和软件设计师的考试标准还实现了中韩互认，以后还将扩大考试互认的级别以及互认的国家。

本考试分 5 个专业类别：计算机软件、计算机网络、计算机应用技术、信息系统和信息服务。每个专业又分 3 个层次：高级资格（高级工程师）、中级资格（工程师）、初级资格（助理工程师、技术员）。对每个专业、每个层次，设置了若干个资格（或级别）。

考试合格者将颁发由人力资源和社会保障部、工业和信息化部用印的计算机技术与软件专业技术资格（水平）证书。

本考试每年分两次举行。每年上半年和下半年考试的级别不尽相同。考试大纲、指定教材、辅导用书由全国计算机专业技术资格考试办公室组编陆续出版。

关于考试的具体安排、考试用书、各地报考咨询联系方式等都在网站 www.ruankao.org.cn 公布。在该网站上还可以查询证书的有效性。

信息安全工程师考试大纲

一、考试说明

1. 考试目标

通过本考试的合格人员能掌握信息安全的知识体系；能够根据应用单位的信息安全需求和信息基础设施结构，规划设计信息安全方案，并负责单位信息系统安全设施的运行维护和配置管理；能够对信息系统运行安全风险和信息设备的安全风险进行监测和分析，并处理一般的安全风险问题，对于重大安全风险问题能够提出整改建议；能够协助相关部门对单位的信息系统进行安全审计和安全事件调查；能够对信息系统和网络安全事件进行关联分析、应急处理，并撰写处理报告；具有工程师的实际工作能力和业务水平。

2. 考试要求

- (1) 熟悉信息安全的基本知识；
- (2) 熟悉计算机网络、操作系统、数据库管理系统的基本知识；
- (3) 熟悉密码学的基本知识与应用技术；
- (4) 掌握计算机安全防护与检测技术；
- (5) 掌握网络安全防护与处理技术；
- (6) 熟悉数字水印在版权保护中的应用技术；
- (7) 了解信息安全相关的法律法规、管理规定；
- (8) 了解信息安全标准化知识；

(9) 了解安全可靠的软硬件平台的基础知识、集成技术和基础应用；

(10) 了解云计算、物联网、互联网、工业控制、大数据等领域的安全管理、安全技术集成及应用解决方案；

(11) 熟练阅读和正确理解相关领域的英文资料。

3. 考试科目设置

(1) 信息安全基础知识，考试时间为 150 分钟，笔试，选择题；

(2) 信息安全应用技术，考试时间为 150 分钟，笔试，问答题。

二、考 试 范 围

考试科目 1：信息安全基础知识

1. 信息安全基本知识

1.1 信息安全概念

- 了解网络空间的概念、网络空间安全学科的内涵、网络空间安全学科的主要研究方向与研究内容

1.2 信息安全法律法规

1.2.1 我国立法与司法现状

- 了解中华人民共和国国家安全法、保密法、网络安全法
- 熟悉中华人民共和国计算机信息系统安全保护条例

1.2.2 计算机和网络安全的法规规章

- 熟悉我国《刑法》对计算机犯罪的规定
- 熟悉我国网络与信息安全相关的法律责任

1.3 信息安全管理基础

1.3.1 信息安全管理制度与政策

- 熟悉我国计算机信息系统等级保护制度
- 了解我国涉及国家秘密的信息系统分级保护制度
- 了解我国密码管理政策
- 了解我国信息安全产品管理政策
- 了解我国互联网信息服务管理政策

1.3.2 信息安全风险评估与管理

- 了解风险分析、评估和风险管理的基本知识

1.4 信息安全标准化知识

1.4.1 熟悉信息安全技术标准的基本知识

1.4.2 了解标准化组织

1.4.3 信息安全系列标准

- 了解信息安全管理标准
- 了解信息安全技术与工程标准

1.5 信息安全专业英语

- 阅读信息安全有关英文资料
- 掌握本领域的基本英语词汇

2. 计算机网络基础知识

2.1 计算机网络的体系结构

2.2 Internet 协议

2.2.1 网络层协议

- 掌握 IP、ICMP、OSPF、RIP、ARP 和 IGMP 协议

- 熟悉 BGP 协议

2.2.2 传输层协议

- 掌握 TCP 和 UDP 协议

2.2.3 应用层协议

- 掌握 DNS、SMTP、POP3、PGP、FTP、HTTP 和 DHCP 协议

3. 密码学

3.1 密码学的基本概念

3.1.1 密码学定义

- 掌握密码的安全目标

3.1.2 密码体制

- 掌握密码技术的基本思想
- 掌握基本的密码体制
- 了解密码分析

3.1.3 古典密码

- 熟悉古典密码的主要编制方法

3.2 分组密码

3.2.1 分组密码的概念

3.2.2 DES

- 熟悉 DES 和 3DES 密码算法
- 了解 DES 和 3DES 的应用

3.2.3 AES

- 熟悉 AES 密码算法
- 了解 AES 密码的应用

3.2.4 SM4

- 熟悉 SM4 密码算法
- 了解 SM4 密码的应用

3.2.5 分组密码工作模式

- 熟悉分组密码工作的 ECB/CBC/CFB/OFB/CTR 模式

3.3 序列密码

3.3.1 序列密码的概念

3.3.2 线性移位寄存器序列

- 熟悉线性移位寄存器序列的概念
- 了解线性移位寄存器序列的应用

3.3.3 RC4

- 熟悉 RC4 密码算法
- 了解 RC4 密码的应用

3.3.4 ZUC

- 熟悉 ZUC 密码
- 了解 ZUC 密码的应用

3.4 Hash 函数

3.4.1 Hash 函数的概念

- 掌握 Hash 函数的概念
- 熟悉 Hash 函数的应用

3.4.2 SHA 算法

- 了解 SHA 算法系列
- 了解 SHA 算法的安全性

3.4.3 SM3 算法

- 熟悉 SM3 算法
- 了解 SM3 算法的应用

3.4.4 HMAC

- 熟悉消息认证码的概念及应用
- 熟悉使用 HMAC 的消息认证码

- 熟悉基于 SM3 的 HMAC

3.5 公钥密码体制

3.5.1 公钥密码的概念

3.5.2 RSA 密码

- 熟悉 RSA 密码算法
- 了解 RSA 密码的特点与应用

3.5.3 ElGamal 密码

- 熟悉 ElGamal 密码算法
- 了解 ElGamal 密码的特点与应用

3.5.4 椭圆曲线密码

- 了解椭圆曲线的概念
- 了解椭圆曲线上的 ElGamal 密码体制

3.5.5 SM2 椭圆曲线公钥加密算法

- 了解 SM2 椭圆曲线公钥加密算法、特点和应用

3.6 数字签名

3.6.1 数字签名的概念

- 掌握数字签名的概念和应用

3.6.2 典型数字签名体制

- 熟悉 RSA 签名算法
- 熟悉 ElGamal 签名算法
- 了解椭圆曲线密码数字签名

3.6.3 SM2 椭圆曲线数字签名算法

- 了解 SM2 椭圆曲线数字签名算法和应用

3.7 认证

3.7.1 认证的概念

3.7.2 身份认证

- 熟悉口令和指纹识别

3.7.3 报文认证

- 熟悉报文源和报文宿的认证
- 熟悉报文内容的认证

3.8 密钥管理

3.8.1 密钥管理的概念

3.8.2 对称密码的密钥管理

- 熟悉对称密钥的生成、分发和存储

3.8.3 非对称密码的密钥管理

- 熟悉非对称密钥的生成
- 熟悉公钥基础设施（PKI）
- 熟悉公钥证书

4. 网络安全

4.1 网络安全的基本概念

- 熟悉基本安全属性
- 了解网络安全事件
- 了解影响网络安全的因素

4.2 网络安全威胁

4.2.1 威胁来源和种类

- 了解网络安全威胁的来源
- 了解网络安全的基本攻击面
- 熟悉网络监听
- 熟悉口令破解
- 熟悉网络钓鱼
- 熟悉网络欺骗
- 了解社会工程
- 熟悉漏洞攻击
- 熟悉恶意代码攻击（僵尸网络）

- 了解供应链攻击

4.2.2 网站安全威胁

- 熟悉 SQL 注入攻击
- 熟悉 XSS
- 熟悉 CSRF
- 熟悉目录遍历威胁
- 了解文件上传威胁

4.2.3 无线网络安全威胁

- 了解无线网络安全威胁的来源
- 熟悉无线网络安全的基本攻击面

4.3 网络安全防御

4.3.1 网络安全防御原则

- 了解最小权限原则、纵深防御原则、防御多样性原则、防御整体性原则、安全性与代价平衡原则、网络资源的等级性原则等

4.3.2 基本防御技术

- 熟悉防火墙技术
- 熟悉入侵检测技术
- 熟悉 VPN 技术
- 熟悉网络容错技术
- 熟悉安全漏洞扫描技术
- 了解网络蜜罐技术
- 了解匿名网络

4.3.3 安全协议

- 熟悉 IPSec 协议、SSL 协议、PGP 协议、TLS 协议、IEEE802.1x 协议、RADIUS 协议、Kerberos 协议、X.509 协议、S/MIME 协议、SSH 协议等

4.4 无线网络安全

4.4.1 无线网络基本知识

- 了解无线广域网、无线城域网、无线局域网和无线个域网概念
- 了解无线传感器网络概念
- 了解无线网状网概念

4.4.2 无线网络安全威胁及分析

- 了解无线网络安全威胁
- 熟悉无线网络安全需求分析
- 熟悉无线网络安全方案设计策略

4.4.3 无线网络安全机制

- 熟悉无线公开密钥体系（WPKI）
- 熟悉有线等效保密协议（WEP）
- 熟悉 Wi-Fi 网络安全接入协议（WPA/WPA2）
- 熟悉无线局域网鉴别与保密体系（WAPI）
- 熟悉 802.11i 协议
- 了解移动通信系统安全机制
- 了解无线传感器网络安全机制
- 了解无线个域网安全机制

5. 计算机安全

5.1 计算机设备安全

5.1.1 计算机安全的定义

- 熟悉计算机安全的属性
- 了解可靠性度量方法

5.1.2 计算机系统安全模型与安全方法

- 熟悉系统安全的概念
- 熟悉系统安全策略的基本模型

- 了解系统安全的实现方法

5.1.3 电磁泄露和干扰

- 了解电磁泄露检测方法和安全防护
- 了解电磁泄露的处理方法

5.1.4 物理安全

- 了解场地安全、设备安全和介质安全

5.1.5 计算机的可靠性技术

- 熟悉容错的基本概念
- 了解硬件容错、软件容错和数据容错

5.2 操作系统安全

5.2.1 操作系统安全基本知识

- 熟悉安全操作系统概念
- 熟悉操作系统安全概念
- 熟悉操作系统的安全性概念

5.2.2 操作系统面临的安全威胁

5.2.3 安全模型

- 掌握 BLP 模型
- 熟悉 Biba 模型、Clark-Wilson 模型、RBAC 模型、DTE 模型、BN 模型

5.2.4 操作系统的安全机制

- 熟悉标识与鉴别机制
- 熟悉访问控制机制
- 熟悉最小特权管理机制
- 熟悉可信通路机制
- 熟悉安全审计机制
- 熟悉存储保护、运行保护和 I/O 保护机制

5.2.5 操作系统安全增强的实现方法

- 了解安全操作系统的设计原则、实现方法和一般开发过程
- 了解操作系统的安全增强技术

5.3 数据库系统的安全

5.3.1 数据库安全的概念

5.3.2 数据库安全的发展历程

5.3.3 数据库访问控制技术

- 熟悉数据库安全模型
- 熟悉数据库安全策略的实施

5.3.4 数据库加密

- 熟悉数据库加密概念
- 熟悉数据库加密技术的基本要求
- 掌握数据库加密技术与访问控制技术的关系

5.3.5 多级安全数据库

- 了解安全数据库标准
- 了解多级安全数据库的体系结构

5.3.6 数据库的推理控制问题

- 了解推理通道分类、产生的原因和解决手段

5.3.7 数据库的备份与恢复

- 熟悉数据库备份
- 了解数据库恢复

5.4 恶意代码

5.4.1 恶意代码定义与分类

- 掌握恶意代码的定义和特征

5.4.2 恶意代码的命名规则

- 了解常用恶意代码前缀解释
- 了解 CARO 命名规则

5.4.3 计算机病毒

- 掌握计算机病毒的定义和特点
- 熟悉计算机病毒的生命周期和传播途径

5.4.4 网络蠕虫

- 掌握网络蠕虫的定义

5.4.5 特洛伊木马

- 掌握特洛伊木马的定义
- 熟悉远程控制型木马的连接方式及其特点
- 熟悉远程控制型木马的常见控制功能、具体用途及其自我隐藏方式

5.4.6 后门

- 掌握后门的定义

5.4.7 其他恶意代码

- 熟悉 DDos、Bot、Rootkit、Exploit 黑客攻击程序、简单软件、广告软件的定义

5.4.8 恶意代码的清除方法

- 熟悉恶意代码对主机的篡改行为
- 熟悉恶意代码的清除步骤

5.4.9 典型反病毒技术

- 熟悉特征值查毒法
- 熟悉校验和技术
- 熟悉启发式扫描、虚拟机技术、行为监控技术、主动防御技术

5.5 计算机取证

5.5.1 计算机取证的基本概念

- 熟悉计算机取证的定义、作用与目的

5.5.2 电子证据及特点

- 熟悉电子证据的定义和特征

5.5.3 计算机取证技术

- 熟悉计算机取证步骤
- 熟悉计算机取证分析技术

5.6 嵌入式系统安全

5.6.1 智能卡安全基础知识

- 掌握智能卡的基本概念
- 了解智能卡相关标准
- 掌握智能卡安全问题与应对策略

5.6.2 USB Key 技术

- 掌握 USB Key 身份认证原理
- 熟悉 USB Key 身份认证的特点
- 掌握 USB Key 的安全问题与应对策略

5.6.3 移动智能终端

- 了解移动智能终端软硬件系统
- 熟悉移动智能终端面临的安全问题及解决途径

5.6.4 熟悉工控系统安全问题及解决途径

5.7 云计算安全

5.7.1 云计算安全基础知识

- 掌握云计算的基本概念
- 了解云计算的 SPI 模型
- 了解云计算面临的信息安全威胁
- 掌握云计算安全的基本概念
- 熟悉云计算安全的相关标准

5.7.2 IaaS 层安全技术

- 掌握虚拟机监控器的概念
- 了解虚拟机监控器和虚拟机实例的安全风险及相关安全技术

- 熟悉虚拟网络的安全
- 熟悉数据存储的安全

5.7.3 PaaS 层安全技术

- 掌握容器的概念
- 了解容器安全技术

5.7.4 SaaS 层安全技术

- 掌握多租户的概念
- 了解应用安全隔离技术

6. 应用系统安全

6.1 Web 安全

6.1.1 Web 安全威胁

- 掌握 Web 安全概念
- 熟悉 Web 安全分类

6.1.2 Web 安全威胁防护技术

- 熟悉 Web 访问安全和 Web 内容安全
- 熟悉网页防篡改技术

6.2 电子商务安全

6.2.1 电子商务安全基础知识

- 熟悉电子商务安全概念、特点和需求

6.2.2 电子商务的安全认证体系

- 熟悉身份认证技术和数字证书技术

6.2.3 电子商务的安全服务协议

- 了解 SET 协议

- 熟悉 SSL 协议

6.3 信息隐藏

6.3.1 信息隐藏基础知识

- 掌握信息隐藏定义、分类和特点
- 熟悉信息隐藏模型
- 了解信息隐藏常用算法（空域算法、Patchwork 算法、频域算法、压缩域算法、NEC 算法、生理模型算法）
- 了解信息隐藏技术的发展和应用领域

6.3.2 数字水印技术

- 掌握数字水印概念
- 熟悉数字水印的基本原理、分类及模型
- 了解数字水印常用实现方法与算法
- 了解视频水印概念
- 了解数字水印攻击方法和对抗策略

6.4 网络舆情

6.4.1 网络舆情的基本概念

- 掌握网络舆情的定义和意义
- 熟悉网络舆情的表现方式和特点

6.4.2 网络舆情的基本技术

- 熟悉网络舆情的诱发因素、监测技术和预警措施

6.5 隐私保护

6.5.1 隐私保护基础知识

- 掌握隐私保护的基本概念
- 了解隐私保护目标
- 熟悉隐私泄露方式

6.5.2 数据挖掘和隐私保护

- 了解数据挖掘与隐私保护的关系

6.5.3 隐私度量与评估标准

- 了解隐私的度量方法
- 了解隐私保护算法的评估标准

考试科目 2：信息安全应用技术

1. 密码学应用

1.1 密码算法的实现

- 了解 DES/3DES 密码算法的软件实现
- 了解 AES 密码算法的软件实现
- 了解 SM4 密码算法的软件实现
- 了解 RC4 密码算法的软件实现
- 了解 SM3 算法的软件实现
- 了解 HMAC 算法的软件实现

1.2 密码算法的应用

1.2.1 典型密码算法的应用

- 熟悉数据加密的基本方法
- 熟悉文件加密的基本方法
- 熟悉通信加密的基本方法

1.2.2 分组密码工作模式

- 熟悉分组密码工作的 ECB/CBC/CFB/OFB/CTR 模式
- 熟悉填充法

1.2.3 公钥密码应用

- 熟悉公钥密码的加密应用

- 了解 SM2 公钥密码在加密和数字签名方面的应用
- 熟悉数字签名的应用

1.3 认证协议的应用

1.3.1 身份认证

- 掌握安全口令技术

1.3.2 典型认证协议的应用

- 熟悉站点认证技术
- 熟悉报文源和报文宿的认证技术
- 熟悉报文内容的认证技术
- 熟悉消息认证码的应用

1.4 密钥管理技术

- 熟悉对称密码会话密钥的产生和分发
- 掌握公钥基础设施和数字证书的应用

2. 网络安全工程

2.1 网络安全需求分析与基本设计

- 熟悉网络安全需求分析
- 熟悉网络安全设计原则

2.2 网络安全产品的配置与使用

2.2.1 网络流量监控和协议分析

- 熟悉网络流量监控的工作原理
- 掌握网络协议分析工具的基本配置

2.2.2 网闸的配置与使用

- 熟悉安全网闸的工作原理
- 掌握安全网闸的基本配置
- 掌握安全网闸的功能配置与使用

2.2.3 防火墙的配置与使用

- 熟悉防火墙的工作原理
- 掌握防火墙的基本配置
- 熟悉防火墙的策略配置

2.2.4 入侵检测系统的配置与使用

- 熟悉入侵检测系统的工作原理
- 掌握入侵检测系统的基本配置
- 熟悉入侵检测系统的签名库配置与管理

2.3 网络安全风险评估实施

2.3.1 基本原则与流程

- 熟悉基本原则和基本流程

2.3.2 识别阶段工作

- 熟悉资产识别
- 熟悉威胁识别
- 熟悉脆弱性识别

2.3.3 风险分析阶段工作

- 熟悉风险分析模型
- 熟悉风险计算方法
- 熟悉风险分析与评价
- 熟悉风险评估报告

2.3.4 风险处置

- 熟悉风险处置原则
- 熟悉风险整改建议

2.4 网络安全防护技术的应用

2.4.1 网络安全漏洞扫描技术及应用

- 熟悉网络安全漏洞扫描的工作原理

- 熟悉网络安全漏洞扫描器分类
- 掌握网络安全漏洞扫描器的应用
- 熟悉网络安全漏洞的防御

2.4.2 VPN 技术及应用

- 熟悉基于虚拟电路的 VPN
- 熟悉应用层 VPN
- 熟悉基于隧道协议的 VPN
- 熟悉基于 MPLS 的 VPN

2.4.3 网络容灾备份技术及应用

- 熟悉网络容灾备份系统的工作原理
- 熟悉网络容灾备份系统的分类
- 掌握网络容灾备份系统的应用

2.4.4 日志分析

- 熟悉日志分析的基本原理
- 掌握日志分析方法
- 掌握日志分析应用

3. 系统安全工程

3.1 访问控制

3.1.1 访问控制技术

- 掌握基于角色的访问控制技术
- 熟悉 Kerberos 协议

3.1.2 身份认证技术

- 熟悉口令猜测技术
- 了解常用网站口令强度分析技术

3.2 信息系统安全的需求分析与设计

3.2.1 信息系统安全需求分析

- 熟悉信息系统安全需求
- 熟悉安全信息系统的构建过程

3.2.2 信息系统安全的设计

- 熟悉信息系统安全体系
- 掌握信息系统安全的开发构建过程和设计方法

3.3 信息系统安全产品的配置与使用

3.3.1 Windows 系统安全配置

- 熟悉用户管理配置、系统管理配置和网络管理配置

3.3.2 Linux 系统安全配置

- 熟悉用户管理配置、系统管理配置和网络管理配置

3.3.3 数据库的安全配置

- 熟悉用户管理配置
- 熟悉数据库管理配置

3.4 信息系统安全测评

3.4.1 信息系统安全测评的基础与原则

- 熟悉信息系统安全测评的内容
- 熟悉信息系统安全测评的基本原则
- 熟悉信息系统安全的分级原则

3.4.2 信息系统安全测评方法

- 熟悉模糊测试
- 熟悉代码审计

3.4.3 信息系统安全测评过程

- 熟悉测评流程
- 熟悉安全评估阶段、安全认证阶段和认证监督阶

段的工作内容

4. 应用安全工程

4.1 Web 安全的需求分析与基本设计

4.1.1 Web 安全威胁

- 熟悉 OWASP Top 10 Web 安全分类

4.1.2 Web 安全威胁防护技术

- 掌握注入漏洞防护技术
- 掌握失效的身份认证和会话管理防护技术
- 掌握跨站脚本（XSS）防护技术
- 熟悉其余常见 Web 安全威胁防护技术

4.2 电子商务安全的需求分析与基本设计

- 熟悉电子商务系统的体系架构
- 熟悉电子商务系统的需求分析
- 熟悉电子商务系统的常用安全架构
- 掌握电子商务系统的常用安全技术

4.3 嵌入式系统的安全应用

4.3.1 嵌入式系统的软件开发

- 熟悉嵌入式的交叉编译环境配置方法
- 了解嵌入式 C 语言的编程方法和编译方法
- 熟悉 IC 卡的安全配置和应用

4.3.2 移动智能终端

- 掌握移动智能终端的主流 OS 的安全防护和配置方法
- 掌握移动智能终端应用安全

4.4 数字水印在版权保护中的应用

- 熟悉数字版权保护系统的需求分析

- 熟悉基于数字水印的数字版权保护系统体系架构
- 掌握数字版权保护系统的常用数字水印技术
- 了解数字版权保护系统的技术标准

4.5 位置隐私保护技术的应用

4.5.1 位置隐私安全威胁

- 熟悉位置隐私保护的需求分析
- 了解位置隐私保护的体系架构
- 掌握位置隐私保护的常用方法

4.5.2 位置隐私 k-匿名模型的算法和应用

- 了解基于空间划分的匿名算法
- 了解基于 Hilbert 值的 k-匿名算法
- 了解基于用户位置的动态匿名算法

三、题 型 举 例

（一）选择题

BLP 模型的设计目标是解决信息系统资源的____（1）____保护。

- （1） A. 不可否认性 B. 机密性
C. 完整性 D. 匿名性

（二）问答题

设现有一个基于 RSA 算法的网络签名协议，基本描述如下：

设 M 为明文， $K_{eA} = \langle e, n \rangle$ 是 A 的公开钥， $K_{dA} = \langle d, p, q, \phi(n) \rangle$ 是 A 的保密的私钥，

A 对的 M 签名过程是,

$$S_A = D(M, K_{dA}) = (M^d) \bmod n$$

S_A 是 A 对 M 的签名。

验证签名的过程是,

$$E(S_A, K_{eA}) = (M^d)^e \bmod n = M$$

问题 1: 请简要描述 RSA 算法的基本思想, 其安全性的基础是什么?

问题 2: 该签名过程是否安全, 如果安全请给出理由, 如果不安全, 请给出反例, 并给出解决思路。